(12) SOLICITUD INTERNACIONAL PUBLICADA EN VIRTUD DEL TRATADO DE COOPERACIÓN EN MATERIA DE PATENTES (PCT)

(19) Organización Mundial de la Propiedad Intelectual
Oficina internacional

(43) Fecha de publicación internacional
3 de Enero de 2002 (03.01.2002)

PCT

(10) Número de Publicación Internacional
WO 02/01793 A1

(51) Clasificación Internacional de Patentes[7]: H04L 9/32, G06F 1/00

(21) Número de la solicitud internacional: PCT/ES01/00250

(22) Fecha de presentación internacional:
22 de Junio de 2001 (22.06.2001)

(25) Idioma de presentación: español

(26) Idioma de publicación: español

(30) Datos relativos a la prioridad:
P 200001646 23 de Junio de 2000 (23.06.2000) ES

(71) Solicitante *(para todos los Estados designados salvo US)*: **ESIGNUS, S.L.** [ES/ES]; Zuatzu Kalea 3, planta 1ª, oficina 2, E-20009 San Sebastian (ES).

(72) Inventores; e

(75) Inventores/Solicitantes *(para US solamente)*: **DE LA PUENTE ARRATE, Fernando** [ES/ES]; Córdoba, 16 7° C, E-35016 Las Palmas de Gran Canaria (ES). **SANDOVAL GONZALEZ, Juan, Domingo** [ES/ES]; Doctor Apolinario Macías, 22 1° 2ª, E-35011 Las Palmas de Gran Canaria (ES).

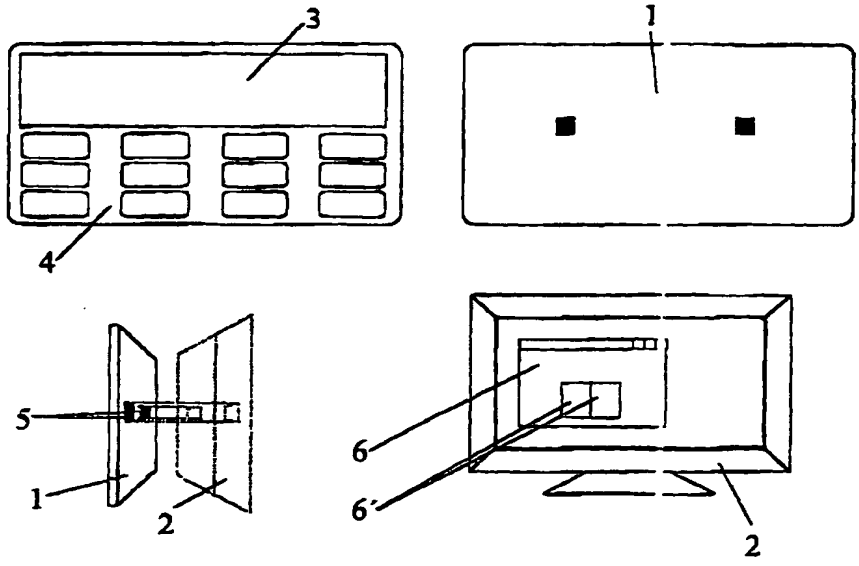
(74) Mandatario: **CARPINTERO LOPEZ, Francisco**; Herrero & Asociados, S.L., Alcalá, 35, E-28014 Madrid (ES).

(81) Estados designados *(nacional)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Continúa en la página siguiente]

(54) Title: EXTERNAL SIGNATURE DEVICE FOR A PC WITH OPTICAL DATA INPUT VIA THE MONITOR

(54) Título: DISPOSITIVO FIRMADOR EXTERNO PARA PC, CON ENTRADA ÓPTICA DE DATOS A TRAVÉS DEL MONITOR



(57) Abstract: The invention relates to a device for electronic signature of data that can be immediately used in electronic banking and electronic commerce or in any other system based on electronic signature. The device has an electronic data input and the data can be received via any computer screen, in addition to a display to show the data to be signed. The device also has a keyboard for interaction with the user and a system for processing the electronic signature. The device is not reprogrammable, which makes it immune to possible attacks by virus or malicious software that could affect the security of the system. Furthermore, the display of data to be signed makes it possible for the user to know what data he or she is actually signing.

[Continúa en la página siguiente]

WO 02/01793 A1

(84) Estados designados *(regional)*: patente ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), patente euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), patente europea (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), patente OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publicada:

— *con informe de búsqueda internacional*

— *enteramente en forma electrónica (excepto para esta página de portada) y disponible por medio de la Oficina Internacional previa petición*

Para códigos de dos letras y otras abreviaturas, véase la sección "Guidance Notes on Codes and Abbreviations" que aparece al principio de cada número regular de la Gaceta del PCT.

(57) Resumen: Se describe un dispositivo para la firma electrónica de datos susceptible de aplicación inmediata en la banca electrónica y en el comercio electrónico, o en cualquier sistema basado en firma electrónica, con entrada óptica de datos para recibirlos a través de cualquier pantalla de ordenador, y con un display para la visualización de los datos a firmar. Además dispone de un teclado para la interacción con el usuario y un sistema para el procesado de la firma electrónica. El dispositivo no es reprogramable, lo que lo hace inmune a posibles ataques de virus o software malicioso que podrían afectar a la seguridad del sistema. Por otro lado, la visualización de los datos a firmar permite al usuario saber realmente qué datos está firmando.

DISPOSITIVO FIRMADOR EXTERNO PARA PC, CON ENTRADA ÓPTICA DE DATOS A TRAVÉS DEL MONITOR

DESCRIPCIÓN

Objeto de la Invención

La presente invención se refiere a un dispositivo firmador externo para PC, con entrada óptica de datos a través del monitor, que aporta esenciales características de novedad y notables ventajas con respecto a los medios conocidos y utilizados para estos mismos fines en el estado actual de la técnica.

Más en particular, la invención propone un dispositivo firmador de tipo universal, susceptible de ser utilizado en combinación con el monitor de cualquier ordenador, mediante el que se proporciona al usuario una transmisión apropiada de los datos a firmar directamente desde la pantalla del monitor, sin que para ello se requiera ningún tipo de instalación o configuración adicional. El sistema aporta características de seguridad operativa altamente incrementadas, puesto que al no ser reprogramable resulta inmune al posible ataque de virus u otro software malicioso, y además permite la utilización de datos alfanuméricos por parte del usuario.

El campo de aplicación de la invención se encuentra comprendido, obviamente, dentro del sector industrial dedicado a la fabricación y/o instalación de sistemas y dispositivos informáticos y de comunicaciones, para la realización de operaciones de comercio electrónico.

Antecedentes de la Invención

La realización de operaciones monetarias (o de cualquier otra índole), de forma remota, en el estado actual de la técnica, presenta el inconveniente de que puede dar origen a indeseada suplantación de identidades. Por ello, es necesario articular mecanismos que permitan autentificar la identidad del ordenante de forma segura. Un método muy utilizado hasta ahora viene siendo la utilización de un nombre de usuario y una palabra secreta de paso que el usuario debe mostrar al otro extremo antes de empezar a operar. Esta información se envía cifrada de forma que nadie más que el destinatario pueda obtener la clave de acceso. El problema de este sistema de autentificación es que al usarse siempre la misma clave de acceso es relativamente fácil de atacar. Otro método de autentificación más robusto consiste en el uso de la firma electrónica. La incorporación de la firma electrónica a las operaciones de comercio electrónico, supone una importante mejora en la seguridad ya que no se usa una única clave de autentificación para cualquier documento, sino que se genera una firma distinta para cada uno. Esta firma es función del ordenante (de la clave de firma que posee el ordenante) y del propio documento. Esto supone que aunque un atacante consiga interceptar un documento junto con su firma no podrá generar la firma correspondiente para otro documento diferente. Existen dos tipos de firma, según al tipo cifrado utilizado: simétrico o asimétrico.

En el cifrado simétrico, se usa la misma clave para firmar y para verificar la firma. Esto supone que tanto el que firma los datos como el que debe verificar la firma deben compartir la clave de firma. De esta forma, sólo ellos serán capaces de firmar u verificar los documentos. Este tipo de firma digital está muy extendido actualmente, pero se pueden presentar problemas sí en

algún momento se requiere que alguien más verifique la firma ya que esto significaría tener que dar a conocer la clave de firma/verificación.

En el cifrado asimétrico, se usan dos claves complementarias, una para firmar y otra para verificar, de forma que lo que se firma con un clave puede ser verificado con la otra. El hecho de disponer de dos claves nos permite mantener en secreto una de ellas (la de firma) y hacer pública la otra (la de verificación). Por otro lado, si se desea realizar una autentificación ante alguien, podremos firmar un bloque de datos con nuestra clave de firma de forma que cualquiera pueda, usando nuestra clave de verificación, verificarla.

Ahora bien, estos sistemas son seguros en la medida que la gestión de las claves sea buena, esto es, que las claves de firma se mantengan fuera del alcance de cualquier atacante y que el mecanismo de publicación de las claves de verificación garantice su integridad. Si las claves de firma se almacenan en ficheros dentro de los ordenadores, existe el peligro de que alguien acceda ilícitamente a estos datos y los copie sin nuestro conocimiento, ya sea de forma local o remota mediante un virus.

Las tarjetas inteligentes resuelven este problema aislando las claves de firma en un dispositivo externo al ordenador, de forma que las claves nunca pueden ser extraídas de la tarjeta, sino que tan sólo se le pueden pasar datos para que los firme. Esto supone un importante avance, ya que garantiza que nadie podrá robar nunca la clave de firma.

Sin embargo, incluso las tarjetas inteligentes

pueden ser atacadas, aunque el ataque en este caso sea algo más sofisticado. Este ataque consiste en usar un virus o un troyano para ordenar operaciones a la tarjeta mientras ésta esté activada sin que el usuario note nada extraño.

De todo esto se puede concluir que no se puede confiar en los ordenadores para llevar a cabo la firma electrónica, ya sea directamente teniendo las claves de firma en el disco duro o a través de tarjetas inteligentes. Por ello, para que el sistema de firma sea seguro es necesario usar hardware no reprogramable y confiable con posibilidad de visualizar los datos a firmar y que requiera la interacción del usuario para realizar las operaciones de firma.

Sumario de la Invención

El sistema asociado al dispositivo que aquí se describe, amplía la funcionalidad de las tarjetas inteligentes, permitiendo al usuario la visualización de estos datos antes de su firma, a efectos de verificación, impidiendo que se firmen datos que el usuario no desea. Es por ello que este dispositivo mejora sustancialmente la seguridad de los sistemas basados en firma electrónica, siendo de aplicación inmediata en la banca electrónica y el comercio electrónico.

Ahora bien, el hecho de usar un dispositivo externo, no reprogramable y con visualización de los datos a firmar, para realizar la firma digital, soluciona el problema de la seguridad, pero añade la necesidad de articular un mecanismo para la introducción de los datos a firmar así como el paso de la firma resultante al ordenador. Una posible solución consiste en hacer que el

usuario introduzca manualmente los datos a firmar a través del teclado del dispositivo externo, el cual genera la firma y la muestra en el visualizador (display) para que el usuario la teclee en el ordenador. Esto supone para el usuario introducir dos veces los mismos datos, primero en el ordenador y posteriormente en el firmador, lo que a menudo resulta poco eficiente, sobre todo cuando el teclado del firmador es pequeño y muy incómodo de usar. Por otro lado, sería posible usar una conexión entre el dispositivo firmador y el ordenador de forma que el usuario únicamente tuviera que comprobar la integridad de los datos y ordenar la generación de la firma de éstos. Sin embargo, esto presenta una complicación añadida si se desea que el firmador sea de uso universal.

El dispositivo objeto de descripción, se caracteriza por solucionar todos estos problemas a la vez, usando un dispositivo de fácil manejo, no reprogramable, con visualización de los datos a firmar y con un sistema de recepción de datos que le permite leer los datos a firmar directamente de la pantalla de cualquier ordenador. Puesto que todos los ordenadores poseen un monitor, podemos considerar que este sistema es universal y que no requiere ningún tipo de instalación o configuración adicional. Una vez transmitidos los datos y generada la firma, el usuario debe introducir manualmente la firma en el ordenador, lo que supone escribir alrededor de cinco caracteres.

Tanto la recepción óptica de los datos, como la introducción manual permiten la selección de la divisa de las magnitudes económicas del documento. Una orden de transferencia bancaria, por ejemplo, se puede realizar en una de las varias divisas disponibles.

El equipo firmador dispone de varias claves de firma. Cada clave está asociada a una autoridad de verificación. De esta forma el mismo equipo se puede usar para autentificar al usuario y firmar documentos para varias entidades independientes entre sí. Por ejemplo, la clave 0 se puede usar para autentificación en la empresa del usuario; la clave 1 para las ordenes, mediante la banca por Internet, a un banco; la clave 2 para las ordenes a un broker para la compra venta de acciones por Internet; ...

El dispositivo más parecido al objeto de esta solicitud de patente que existe actualmente en el mercado consiste en el sistema Digipass de VASCO. Este sistema se diferencia del expuesto en esta descripción en que el sistema Digipass no soporta la recepción y procesado de documentos alfanuméricos, el uso de varias divisas para definir las unidades económicas y la selección de una clave de firma entre varias disponibles. Por otra parte, el sistema Digipass de VASCO es reprogramable, lo que lo hace vulnerable frente a un posible ataque.

En una forma de realización preferida, el dispositivo de la invención incluye cuatro elementos clave, a saber:

- un sistema de recepción de datos óptico, que le permite recibir datos a través de cualquier monitor de ordenador (Tubos de rayos catódicos, TFT y cualquier otra tecnología de visualización);
- un display alfanumérico, que permite la visualización de estos datos así como los menús de opciones propias del dispositivo;

- un teclado para permitir al usuario interactuar con el dispositivo (introducir el PIN, usar los menús de visualización de los datos, y aceptar o cancelar la generación de la firma);

- un sistema e configuración del equipo con el que se pueden definir el PIN de activación, la divisa por defecto, el idioma de los mensajes que se muestran al usuario y la clave de firma por defecto, y

- el sistema de firma que procesa las operaciones de firma de los datos recibidos.

Breve Descripción de los Dibujos

Estas y otras características y ventajas de la invención, se pondrán más claramente de manifiesto a partir de la descripción detallada que sigue de una forma preferida de realización, dada únicamente a título de ejemplo ilustrativo y no limitativo, con referencia a los dibujos que se acompañan, en los que:

La Figura 1 muestra un diagrama esquemático representativo del dispositivo firmador externo según la invención;

La Figura 2 representa un diagrama de bloques ilustrativo del proceso seguido con el dispositivo de la invención;

La Figura 3 es una representación simplificada de la forma de la señal recibida desde un monitor CRT, una vez filtradas las componentes de alta frecuencia;

La Figura 4 ilustra la forma de la señal cuando se

recibe desde un monitor TFT, y

La Figura 5 muestra, de forma esquematizada, el proceso relativo a la criptografía de clave privada utilizada para la implementación de la firma electrónica.

Descripción de una Forma de Realización Preferente

La descripción detallada de la forma de realización preferente de la presente invención va a ser efectuada en lo que sigue con referencia a los dibujos anexos, cuya Figura 1 muestra el diseño genérico del firmador externo. Según esta representación, se observa que el dispositivo incluye un sistema óptico 1 para la recepción de datos, en el que se encuentran incorporados los fotodetectores 5 para la detección de las señales ópticas enviadas desde el monitor 2, apareciendo indicada con la referencia numérica 6 el área específica de transmisión desde éste, y pudiendo ser dicho monitor de cualquier tipo apropiado conocido (tubo de rayos catódicos TRC, TFT o cualquier otra tecnología de visualización); por su parte, el display alfanumérico aparece indicado con la referencia numérica 3, mientras que el teclado ha sido indicado con la referencia 4. El sistema de firma destinado a procesar las operaciones de firma de los datos recibidos, no ha sido representado de manera explícita.

El procedimiento usado para la firma con este dispositivo se muestra esquemáticamente en el diagrama de bloques de la Figura 2. En primer lugar se activa el firmador mediante la introducción de un PIN a través del teclado 4, siendo transmitidos a continuación los datos a firmar desde el ordenador 11 hacia el firmador a través del monitor 2. Una vez recibidos correctamente los datos, se visualizan en el display 3 del firmador para que el

usuario compruebe que son correctos. Si es así, el usuario ordenará la firma en la etapa 7 de validación de usuario, pulsando la tecla correspondiente del teclado, y la firma generada en la etapa 8 siguiente se mostrará en el display en la etapa 9. Esta firma estará compuesta por unos pocos caracteres alfanuméricos que el usuario deberá introducir manualmente en el ordenador 11 a través del teclado 10 de este último.

Para facilitar su uso el firmador dispone de una aplicación de configuración que permite cambiar los parámetros. Los parámetros configurables son:

- PIN. Se puede cambiar el PIN de activación del equipo.

- Idioma. Se puede seleccionar un idioma de entre los cuatro programados (euskera, catalán, inglés y castellano).

- Divisa por defecto. Cuando se introducen los datos por teclado, si no se introduce ninguna divisa se tomará ésta. Los valores posibles son: peseta, euro, dólar y libra.

- Clave por defecto. Cuando se introducen los datos por teclado, si no se introduce ninguna clave, se tomará esta.

De acuerdo con lo anterior, la implantación real del sistema se lleva a cabo como sigue:

La operación de recepción óptica se lleva a cabo con el ordenador 11 que ejecuta un programa en el que se convierten los datos a firmar en cambios en la

luminosidad o color de una zona 6 de la pantalla del monitor 2. La transmisión de un bit de datos se realiza con la variación de color de dicha área 6 de transmisión de la pantalla, de modo que, en esta realización, el color negro equivale a la transmisión de un cero, mientras que el color blanco representa un uno.

Ahora bien, cuando se trabaja con sistemas operativos multitarea, se debe tener en cuenta el hecho de que el procesador es compartido por múltiples procesos, algunos a nivel de aplicación y otros a nivel de sistema operativo. Esto implica que no se puede garantizar que el programa se ejecute de forma síncrona por lo que puede ocurrir que el tiempo en el que se muestra un bit en pantalla varíe considerablemente. Esto conlleva una cierta incertidumbre cuando el color del área 6 de transmisión no varía durante varios ciclos consecutivos, ya que esto puede significar dos cosas: que se esté transmitiendo a una secuencia de varios bits a cero o varios bits a uno, o que el administrador de procesos del sistema operativo haya pasado el control del procesador a otro proceso, en cuyo caso la transmisión se suspende hasta que el proceso transmisor recupera el control del procesador. Para solucionar este problema se debe generar también una señal de reloj que indique al firmador cuando debe muestrear la señal para recuperar un bit.

La solución consiste en usar dos zonas diferenciadas de la pantalla, referenciadas como D (derecha) e I (izquierda), las cuales aparecen claramente representadas en el monitor 2 de la figura 1, y referenciados con el 6´. El cuadro D se usa para transmitir datos, mientras que el cuadro I se emplea para enviar una secuencia de sincronismo que permita diferenciar los estados de

inactividad y la transmisión de varios bits repetidos. Por lo tanto, el sistema receptor deberá disponer de dos fotodetectores 5, uno para leer los datos transmitidos desde el cuadro D, y el otro para recibir una secuencia de sincronismo. Cada una de estas entradas lleva un filtro RC (no representado) que elimina las componentes de alta frecuencia de la señal debidas al barrido horizontal en el caso de los monitores con tubos de rayos catódicos.

Otro aspecto muy importante, consiste en la posibilidad de trabajar con todo tipo de monitores, independientemente de la tecnología que estos usen. Estas tecnologías pueden dividirse en dos grandes grupos: a)un primer grupo en el que la imagen se actualiza a intervalos regulares (ciclo de refresco), y b) un segundo grupo en el que la señal se mantiene invariable hasta que se produce un cambio de color en la imagen a mostrar. En el primer grupo (monitores con rayos catódicos, CRT), la señal recibida está formada por una componente principal de baja frecuencia (frecuencia de refresco de la pantalla), y una componente añadida de alta frecuencia causada por el barrido horizontal del haz de rayos catódicos sobre la pantalla. Por el contrario, la señal recibida desde un monitor TFT es estable durante todo el tiempo de bit, observándose tan sólo una pendiente de subida o de bajada en las transiciones entre la transición de un cero y un uno y viceversa. Además, se observa que al permanecer constante la señal durante todo el tiempo de bit, la intensidad instantánea es menor que en el caso de los CRT en los que la intensidad se concentra en un corto intervalo de tiempo inferior al ciclo de refresco. Esto lleva a la necesidad de tratar ambos casos de forma separada, para lo cual se debe detectar, en primer lugar, el tipo de monitor desde el

que se transmiten los datos. Para ello se hace uso de una secuencia inicial de tres bits (111) que se traduce en la secuencia (B,B) (B,N) (B, B).

La figura 3 muestra, de forma simplificada el aspecto de la señal recibida desde un monitor CRT, una vez filtrada las componentes de alta frecuencia. En el gráfico que aparece en esta figura, se ha representado la intensidad (I) de luz (eje de ordenadas)en función del tiempo (t), correspondiendo los primeros ciclos al color blanco y los dos segundos al color negro. En los dos primeros ciclos correspondientes al color blanco, se puede apreciar la elevación del nivel correspondiente a la intensidad luminosa, durante una parte del periodo correspondiente al ciclo de refresco, donde se verifica la persistencia del color.

Por su parte, la figura 4 muestra, por el contrario, la forma de la señal recibida desde un monitor TFT. La representación corresponde asimismo con la variación de la intensidad (I) de luz en función del tiempo (t), apareciendo representados cuatro ciclos de duración equivalente al período de la señal de refresco, de los que los dos primeros ciclos, de mayor nivel, corresponden al color blanco, y los dos segundos corresponden al color negro.

En lo que se refiere a la implementación de la firma electrónica, debe tenerse en cuenta que los sistemas de firma electrónica usados actualmente hacen uso de la criptografía de clave pública, lo que conlleva la necesidad de poder restaurar el mensaje firmado a partir de los datos cifrados con la clave privada. Esto hace que el tamaño de los datos cifrados sea al menos igual al de los datos firmados, ya que de no ser así se perdería

información a lo largo del proceso de firma. Más aún, los sistemas de clave pública usados actualmente generan una firma de tamaño igual al de las claves usadas para cifrar y descifrar el extracto del mensaje, obteniéndose así una firma de 512, 1024 o 2048 bits. Esto supone un grave problema para el usuario que debe copiar manualmente esta información al ordenador con el esfuerzo que esto supone y la alta probabilidad de equivocarse al copiar los datos. Por ello es conveniente hallar un sistema que permita firmar documentos generando una firma de tamaño reducido sin que esto suponga una reducción en la seguridad del sistema.

El método de firma que se utiliza con el dispositivo que aquí se describe, resuelve también este inconveniente, puesto que se basa en la criptografía de clave privada, usando como firma electrónica los primeros 3 a 6 bytes de los datos cifrados con la clave privada, según aparece representado en el diagrama esquemático de la Figura 5, en el que un bloque 12 representa los datos a firmar, un bloque 13 representa el modo de cifrado simétrico con la utilización de una clave 16, y un bloque 14 representa el resultado del cifrado, con una parte rayada a la izquierda de este bloque, indicativa de la parte de cifrado utilizada como firma. El hecho de usar tan sólo una parte 15 de la salida del cifrado como firma, no aumenta las posibilidades de ataque del sistema. Por el contrario, lo único que supone es que un posible atacante dispondrá de menos información para poder realizar el ataque, ya sea por fuerza bruta o por métodos cripto-analíticos.

Para mostrar la firma en el display 3 se codifica la firma agrupando los bits de 6 en 6. Seis bits generan 64 valores posibles y se mapean al siguiente conjunto: `-´,

`+´, `0´ al `9´, `a´ a la `z´ y `A´ a `Z´ (tabla ASCII).

Por último, en lo que se refiere a la implementación del software de transmisión para ordenador, encargado de transmitir los datos a firmar desde el PC hacia el firmador externo, debe poder sincronizarse con el refresco de pantalla de la tarjeta gráfica del ordenador con el fin de enviar un bit de datos en cada ciclo de refresco. Para ello se hace uso de las librerías gráficas DirectX (para sistemas operativos tales como Windows) y OpenGL (para plataformas Unix).

En este sentido, existen dos posibles implementación, a saber, como una aplicación independiente que implemente el sistema de transmisión así como todo el interfaz de usuario, o como un componente añadido a otra aplicación (principalmente un navegador Web), como es el caso de los ActiveX y los plug-ins, de forma que tan sólo es necesario implementar el código para realizar la transmisión de datos. Estos componentes dispondrían de una interfaz simple con una función de transmitir a la que se le pasen como parámetros los datos a transmitir.

Como se comprenderá fácilmente, el dispositivo de la invención descrito en lo que antecede, es de aplicación inmediata en la banca electrónica y al comercio electrónico, aunque podría ser utilizado en cualquier sistema basado en firma electrónica en el que se requiera un alto grado de seguridad sin que esto suponga ninguna complicación adicional para el usuario, siempre que la cantidad de datos a firmar sea relativamente baja.

No se considera necesario hacer más extenso el contenido de esta descripción para que un experto en la

materia pueda comprender su alcance y las ventajas derivadas de la invención, así como desarrollar y llevar a la práctica el objeto de la misma.

No obstante, debe entenderse que la invención ha sido descrita según una realización preferida de la misma, por lo que puede ser susceptible de modificaciones sin que ello suponga alteración alguna del fundamento de dicha invención, pudiendo afectar tales modificaciones tanto a las características constructivas como operativas de conjunto, según se define mediante las reivindicaciones anexas.

REIVINDICACIONES

1.- Dispositivo firmador externo para PC, con entrada óptica de datos a través del monitor, susceptible de aplicación inmediata en la banca electrónica y el comercio electrónico, o en cualquier otro sistema basado en firma electrónica en el que se requiera un alto grado de seguridad con una cantidad de datos a firmar relativamente baja, que se caracteriza porque dicho dispositivo incluye un sistema óptico (1) de recepción de datos desde un monitor (2) de ordenador; un visualizador (3) o display alfanumérico, para la visualización de los datos a firmar; un teclado (4) para la interacción del usuario con el dispositivo, y un sistema de firma encargado de procesar las operaciones de firma de los datos recibidos.

2.- Dispositivo firmador según la reivindicación 1, que se caracteriza por la povisión de una zona (6) en el monitor (2) para la transmisión de datos al detector óptico (1), en la que se han determinado dos secciones (6, 6') de las que una primera sección se encarga de enviar datos y la otra sección se encarga de enviar una secuencia de sincronismo mediante la que se diferencian los estados de inactividad y los de transmisión de varios bits repetidos, incorporando además dicho sistema óptico (1) de recepción elementos fotodetectores 85) para la detección de las señales enviadas desde las secciones (6') en correspondencia con las variaciones de luz experimentadas por el dispositivo de visualización que se utilice.

3. Dispositivo firmador según la reivindicación 1 ó 2, que se caracteriza porque no es susceptible de re-programación, y porque su activación se realiza mediante

la introducción de un número de identificación personal (PIN).

4. Dispositivo firmador según una o más de las reivindicaciones 1 a 3 anteriores, que se caracteriza por la capacidad de mostrar la firma en el display (3) para que sea copiada en el equipo destino, siendo dicha firma generada con la utilización de un algoritmo criptográfico que utiliza la misma clave para firmar y para verificar dicha firma, pudiendo contener los documentos a firmar cualquier carácter alfanumérico, y siendo los datos a firmar susceptibles de introducción mediante teclado, disponiendo el firmador de la posibilidad de acceder a todos los mensajes en varios idiomas.

5. Dispositivo firmador según una o más de las reivindicaciones anteriores, que se caracteriza por la incorporación de un algoritmo de generación de firma abreviada, de tipo criptográfico con forma simétrica (es decir, con la utilización de la misma clave para cifrar y para descrifar), estando la firma compuesta por un subconjunto de los bits generados en el proceso de cifrado, efectuándose el proceso de verificación de firma volviendo a cifrar los datos y comparando los bits de firma con sus homólogos generados en el proceso de verificación, y siendo codificada la firma en subconjuntos de 6 bits con el fin de poder mapearla a un subconjunto de los caracteres ASCII imprimibles.

6. Dispositivo firmador según una o más de las reivindicaciones anteriores, que se caracteriza por la posibilidad de seleccionar una, de entre varias, divisa para las magnitudes monetarias de los documentos a firmar; la posibilidad de seleccionar una, de entre varias, clave de firma; y la posibilidad de seleccionar

uno de entre varios idiomas para la presentación de los mensajes al usuario.

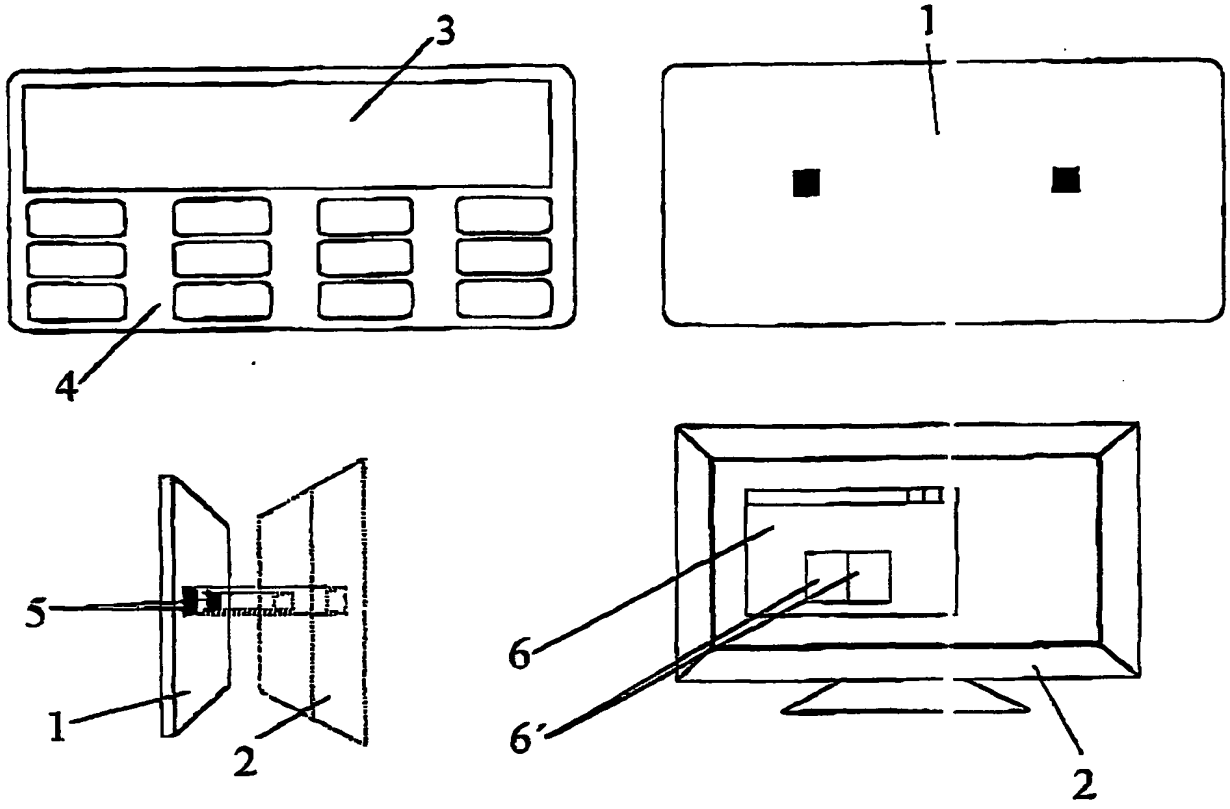


FIG.1

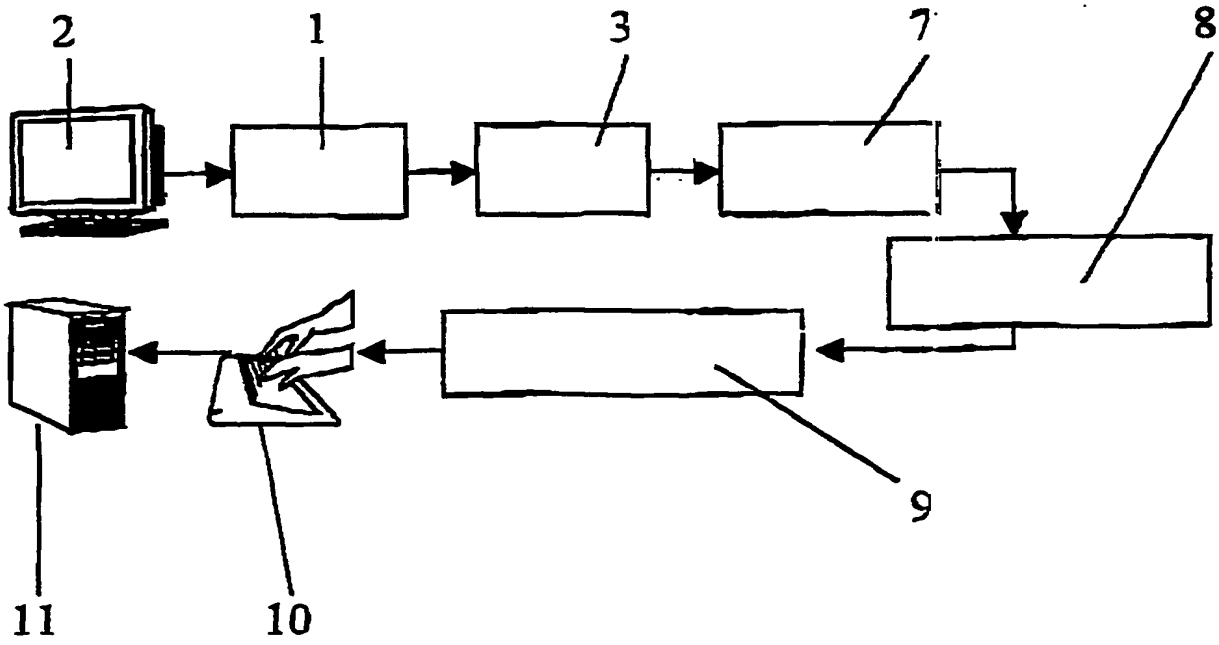


FIG. 2

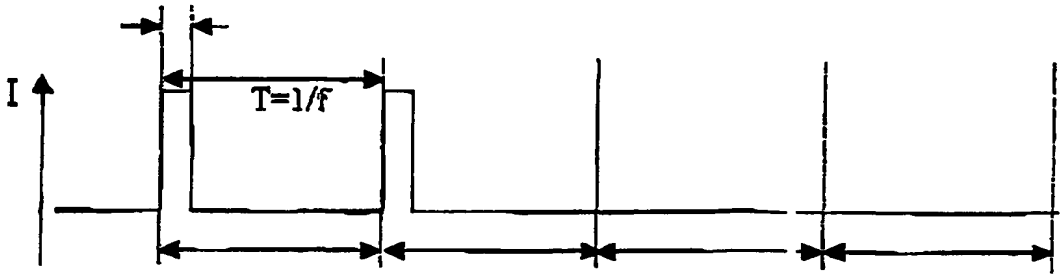


FIG. 3

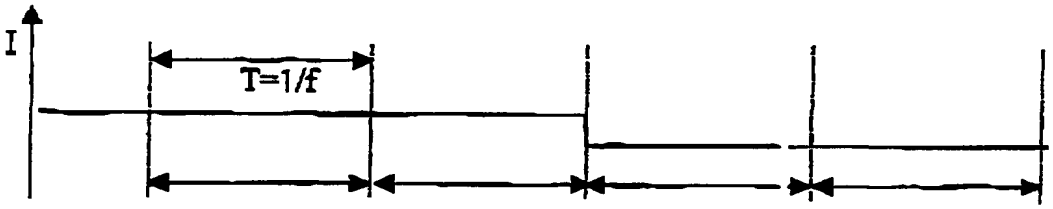


FIG. 4

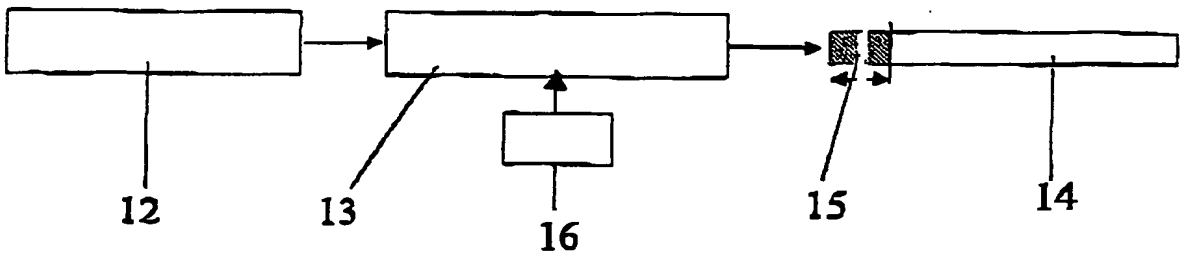


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ES 01/00250

A. CLASSIFICATION OF SUBJECT MATTER

CIP[7] H04L9/32; G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

CIP[7] H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC, WPI,PAJ,INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PA	EP1056014 A1(HEWLEWTT-PACKARD COMPANY) 29 November 2000 (29.11.00), The whole document	1,3
PA	EP1055989 A1(HEWLETT-PACKARD COMPANY) 29 November 2000 (29.11.00), The whole document	1,3
A	DE19811720 A1(KOBIL COMPUTER) 30 September 2000 (30.09.00)	1

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 August 2001	3 October 2001
Name and mailing address of the ISA/ S.P.T.O Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No
PCT/ES 01/00250

Patent document cited in search report	Publication date	Patent familiy member(s)	Publication date
EP1056014 A1	29.11.2000	WO0073913 A1	07.12.2000
EP1055989 A1	29.11.2000	WO0073879 A1	07.12.2000
DE19811720 A1	30.09.1999	NONE	NONE

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional nº
PCT/ES 01/[redacted]

A. CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD

CIP[7] H04L9/32; G06F1/00
De acuerdo con la Clasificación Internacional de Patentes (CIP) o según la clasificación nacional y la CIP.

B. SECTORES COMPRENDIDOS POR LA BÚSQUEDA

Documentación mínima consultada (sistema de clasificación, seguido de los símbolos de clasificación)

CIP[7] H04L, G06F

Otra documentación consultada, además de la documentación mínima, en la medida en que tales documentos formen parte de los sectores comprendidos por la búsqueda

Bases de datos electrónicas consultadas durante la búsqueda internacional (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

EPODOC, WPI,PAJ,INSPEC

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría*	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones nº
PA	EP1056014 A1(HEWLEWTT-PACKARD COMPANY) 29.11.2000, todo el documento	1,3
PA	EP1055989 A1(HEWLETT-PACKARD COMPANY) 29.11.2000, todo el documento	1,3
A	DE19811720 A1(KOBIL COMPUTER) 30.09.1999, todo el documento	1

☐ En la continuación del recuadro C se relacionan otros documentos ☒ Los documentos de familia de patentes se indican en el anexo

* Categorías especiales de documentos citados:

"A" documento que define el estado general de la técnica no considerado como particularmente relevante.

"E" solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior.

"L" documento que puede plantear dudas sobre una reivindicación de prioridad o que se cita para determinar la fecha de publicación de otra cita o por una razón especial (como la indicada).

"O" documento que se refiere a una divulgación oral, a una utilización, a una exposición o a cualquier otro medio.

"P" documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.

"T" documento ulterior publicado con posterioridad a la fecha de presentación internacional o de prioridad que no pertenece al estado de la técnica pertinente pero que se cita por permitir la comprensión del principio o teoría que constituye la base de la invención.

"X" documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado.

"Y" documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.

"&" documento que forma parte de la misma familia de patentes.

Fecha en que se ha concluido efectivamente la búsqueda internacional. 10.08.2001	Fecha de expedición del informe de búsqueda internacional 03 OCT 2001
Nombre y dirección postal de la Administración encargada de la búsqueda internacional O.E.P.M. C/Panamá 1, 28071 Madrid, España. nº de fax +34 91 3495304	Funcionario autorizado M. Alvarez Moreno nº de teléfono + 34 91 349 54 95

INFORME DE BÚSQUEDA INTERNACIONAL
Información relativa a miembros de familias de patentes

Solicitud internacional nº
PCT/ES 01/00250

Documento de patente citado en el informe de búsqueda	Fecha de publicación	Miembro(s) de la familia de patentes	Fecha de publicación
EP1056014 A1	29.11.2000	WO0073913 A1	07.12.2000
EP1055989 A1	29.11.2000	WO0073879 A1	07.12.2000
DE19811720 A1	30.09.1999	NINGUNA	NINGUNA